SPECIALISATION AND REDUCTION OF CONTINUED FRACTIONS OF FORMAL POWER SERIES

ALFRED J. VAN DER POORTEN

To Jean–Louis Nicolas in celebration of his sixtieth birthday

Abstract. We discuss and illustrate the behaviour of the continued fraction expansion of a formal power series under specialisation of parameters or their reduction modulo p and sketch some applications of the reduction theorem here proved.

1. Introduction

Given a continued fraction expansion over a function field $\mathbb{K}(X)$ it may happen that a specialisation of incidental parameters leads some partial quotient to acquire infinite coefficients. I point out that in such a case the partial quotient will 'collapse' to a partial quotient of higher degree. Indeed, I illustrate several techniques for manipulating continued fraction expansions to display such a 'collapse' explicitly.

To make sense of the notion "specialisation" the base field $\mathbb{K} = K(t_1, t_2, \dots)$ should be a transcendental extension of some yet more base field K by one or several algebraically independent parameters t_1, t_2, $\dots$. In the sequel K will be supposed to be $\mathbb{Q}$ or some finite field $\mathbb{F}_p$, but our remarks are often more general.

For example, if $Y^2 = (X^2+u)^2 + 4v(X+w)$ viewed as defined over the field K, then studying the continued fraction of Y will have us working over $\mathbb{K}(X)$, where $\mathbb{K} = K(u, v, w)$.

Definition 1. A *specialisation* is a restriction on the generality of the parameters defining $\mathbb{K}$ over K.

For example, taking $u + w^2 = v$ above is a specialisation; so is a parametrisation $u = 1-2t-t^2$, $v = 1-2t$, $w = t$. *A fortiori*, a numerical example is a specialisation.

Our Y above is a formal Laurent series, an element of $\mathbb{K}((X^{-1}))$. Its 'Taylor' coefficients are elements of $\mathbb{K} = K(u, v, w)$. For simplicity, let me suppose $K = \mathbb{Q}$. I say that replacing the base field $\mathbb{Q}$ by some finite field, say $\mathbb{F}_p$ is a reduction of Y. Of course such a reduction may not make sense, because p occurs in the denominator of some Taylor coefficient. If so, I say variously that Y does not have reduction modulo p or has bad reduction at p.

Received by the editors February 1, 2008.

1991 *Mathematics Subject Classification.* Primary 11J70, 11A65, 11J68.

Key words and phrases. continued fraction expansion, formal power series, function field of characteristic zero.

The author was supported in part by a grant from the Australian Research Council.

Furthermore, one sees readily that for the example $Y^2=(X^2+u)^2+4v(X+w)$ reduction modulo 2 either yields $Y=X^2+u$, a polynomial or, for specialisations of u, v, w, may make no sense. In either case I may call the reduction bad, in the former case because under reduction the curve decreases in genus.

Definition 2. A reduction of an element $Y\in\mathbb{K}((X^{-1}))$ modulo $\mathfrak{p}$ is the replacement, if that makes sense, of Y by the corresponding series defined over $\mathbb{K}_\mathfrak{p}((X^{-1}))$. Here $\mathfrak{p}$ is a maximal ideal of the ring of integers $\mathcal{O}_\mathbb{K}$ of $\mathbb{K}$ and $\mathbb{K}_\mathfrak{p}=\mathcal{O}_\mathbb{K}/\mathfrak{p}\mathcal{O}_\mathbb{K}$.

These remarks serve as introduction to the principal result of this note.

Reduction Theorem. *Suppose $F=\sum f_iX^{-i}$ is a formal series in $\mathbb{K}((X^{-1}))$, say with continued fraction expansion $[\,a_0(X)\,,\,a_1(X)\,,\,\ldots\,]$ and thus with convergents given for $h=0,\ 1,\ \ldots$ by the rational functions*

$$r_h(X)=x_h(X)/y_h(X)=[\,a_0(X)\,,\,a_1(X)\,,\,\ldots\,,\,a_h(X)\,].$$

Now denote by $\overline{F}=\sum\overline{f}_iX^{-i}$ some specialisation of F effected by specialising parameters of the field over which F is defined, or a reduction of F. Then the sequence of convergents to $\overline{F}$ is precisely the sequence $\bigl(\overline{r}_h(X)\bigr)$, however listed without *repetition.*

Note here that if some partial quotient a_h has no specialisation (in more blunt words, blows up) then neither do the *continuants* x_h and y_h. Their quotients r_h will nevertheless have a defined specialisation provided only that the specialisation, or reduction, $\overline{F}$ makes sense. In practice, several distinct convergents r_h, r_{h+1}, …, may collapse to the same convergent $\overline{r}_h$ of $\overline{F}$.

A special case of this phenomenon is noted in [3]. Here there is no collapse on reduction modulo 3. Cantor remarks that because all the partial quotients of

$$G_3(X)=\prod_{h=0}^{\infty}\bigl(1+X^{-3^h}\bigr)$$

are linear if G_3 is viewed as defined over $\mathbb{F}_3$ they must also be linear for G_3 defined over $\mathbb{Q}$. Specifically, in that example the partial quotients of G_3 over $\mathbb{Q}$ all have good reduction modulo 3 (as was shown with inappropriate effort in [1]).

2. Proof of the Theorem

For the immediately following see the introduction to [10], alternatively [14]. We recall that if x_h/y_h is a convergent to F then

(1) $$\deg(y_hF-x_h)=-\deg y_{h+1}=-\deg(a_{h+1}y_h+y_{h-1})=-\deg a_{h+1}-\deg y_h$$

and conversely (Proposition 1 of [10]) that if x and y are coprime polynomials then

(2) $$\deg(yF-x)<-\deg y$$

entails x/y is a convergent to F.

To prove the Theorem we need to notice that, even though both continuants $\overline{x}_h$ and $\overline{y}_h$ may blow up, the existence of $\overline{F}$ implies that there is some constant c_h in $\mathbb{K}$ so that both $\overline{c_hx_h}$ and $\overline{c_hy_h}$ exist and not both vanish identically. Then

$$\deg(\overline{c_hy_h}\overline{F}-\overline{c_hx_h}\,)\le\deg(y_hF-x_h)<-\deg y_h\le-\deg\overline{c_hy_h}$$

so if $r_h=x_h/y_h$ is a convergent to F then, by (2), $\overline{c_hx_h}/\overline{c_hy_h}=\overline{r}_h$ is a convergent to $\overline{F}$.

Suppose however that the convergents $\overline{r}_h$, $\overline{r}_{h+1}$, ..., $\overline{r}_{k-1}$ coincide but neither $\overline{r}_{h-1} = \overline{r}_h$, nor $\overline{r}_{k-1} = \overline{r}_k$. To show we have found *all* the convergents to $\overline{F}$ it suffices for us to see that $\overline{r}_h$ and $\overline{r}_k$ are *consecutive* convergents to $\overline{F}$.

However, of course $\overline{r}_h - \overline{r}_k = \overline{r}_{k-1} - \overline{r}_k$. Note that though neither x_{k-1} and y_k, nor x_k and y_{k-1} might have good reduction, necessarily the difference

$$x_{k-1}y_k - x_k y_{k-1} = (-1)^k$$

and so also the product $y_{k-1}y_k$ must have good reduction without requiring any multiplier. Thus

$$\overline{x_{k-1}y_k - x_k y_{k-1}} = \pm 1.$$

Were it otherwise, we would have $\overline{r}_{k-1} = \overline{r}_k$, contrary to hypothesis. Just so then

$$\overline{x_h y_k - x_k y_h} = \pm 1\,,$$

and necessarily $y_h y_k$, has good reduction, proving that there is no convergent to $\overline{F}$ between the convergents $\overline{r}_h$ and $\overline{r}_k$, as required.

3. Continued Fraction Manipulation

The following remarks are intended to show off several lemmata allowing one to manipulate continued fraction expansions in somewhat surprising ways.

In particular we will see by manipulation of continued fractions that the blowing up of a partial quotient in a continued fraction expansion leads to a collapse to higher degree. The point is that, even if there is a blowup of partial quotients under specialisation or reduction, one does not have to re-expand the function. In principle one can obtain the new continued fraction expansion directly from the original expansion.

3.1. One sees readily, mind you with some pain, that

$$\begin{aligned}
(3)\quad F^{-1} &= \big(aX^{-1} + bX^{-2} + cX^{-3} + dX^{-4} + \cdots\cdots\big)^{-1} \\
&= \tfrac{1}{a}X\big(1 + \tfrac{b}{a}X^{-1} + \tfrac{c}{a}X^{-2} + \tfrac{d}{a}X^{-3} + \cdots\big)^{-1} \\
&= \tfrac{1}{a}X\big(1 - \tfrac{b}{a}X^{-1} - \tfrac{c}{a}X^{-2} - \tfrac{d}{a}X^{-3} - \cdots + \tfrac{b^2}{a^2}X^{-2} + \tfrac{2bc}{a^2}X^{-3} + \cdots - \tfrac{b^3}{a^3}X^{-3} - \cdots\big) \\
&= \big(\tfrac{1}{a}X - \tfrac{b}{a^2}\big) + \tfrac{b^2-ac}{a^3}X^{-1}\big(1 - \tfrac{a^2d-2abc+b^3}{a(b^2-ac)}X^{-1} - \cdots\big) \\
&= [\,\tfrac{1}{a}X - \tfrac{b}{a^2}\,,\ \tfrac{a^3}{b^2-ac}X + \tfrac{a^2(a^2d-2abc+b^3)}{(b^2-ac)^2}\ , \ldots].
\end{aligned}$$

However,

$$\begin{aligned}
(4)\quad \big(F - aX^{-1}\big)^{-1} &= \big(bX^{-2} + cX^{-3} + dX^{-4} + \cdots\cdots\big)^{-1} \\
&= \tfrac{1}{b}X^2\big(1 + \tfrac{c}{b}X^{-1} + \tfrac{d}{b}X^{-2} + \cdots\big)^{-1} \\
&= \tfrac{1}{b}X^2\big(1 - \tfrac{c}{b}X^{-1} - \tfrac{d}{b}X^{-2} - \cdots + \tfrac{c^2}{b^2}X^{-2} + \cdots\big)^{-1} \\
&= [\,\tfrac{1}{b}X^2 - \tfrac{c}{b^2}X + \tfrac{c^2-bd}{b^3}\ , \ldots].
\end{aligned}$$

I now show directly that, indeed, the linear partial quotients of the first expansion collapse to a partial quotient of higher degree when a vanishes. To that end I subtract aX^{-1} from the continued fraction expansion of F or, rather — because this turns out to be more convenient to do — I add aX^{-1} to that of $F - aX^{-1}$.

Thus, consider the expansion

$$F = aX^{-1} + [\,0\,,\,\tfrac{1}{b}X^2 - \tfrac{c}{b^2}X + \tfrac{c^2-bd}{b^3}\,,\,\beta\,] = [\,aX^{-1}\,,\,\tfrac{1}{b}X^2 - \tfrac{c}{b^2}X + \tfrac{c^2-bd}{b^3}\,,\,\beta\,]\,.$$

Of course, actually to suggest aX^{-1} *is* a partial quotient is "wash your mouth out" stuff and we will have to work hard to make up for the outrage. We begin with several fairly well known lemmata, and their little known corollaries.

Lemma 3 (Multiplication)**.**

$$B[\,Ca_0\,,\,Ba_1\,,\,Ca_2\,,\,Ba_3\,,\,Ca_4\,,\,\ldots\,] = C[\,Ba_0\,,\,Ca_1\,,\,Ba_2\,,\,Ca_3\,,\,Ba_4\,,\,\ldots\,].$$

This fact is both obvious and fairly well known. Its present felicitous formulation is given by Wolfgang Schmidt [14].

Lemma 4 (Negation)**.**

$$\begin{aligned}[\,\alpha\,,\,A\,,\,B\,,\,\beta\,] &= [\,\alpha\,,\,A\,,\,0\,,\,-1\,,\,1\,,\,-1\,,\,0\,,\,-B\,,\,-\beta\,]\\ &= [\,\alpha\,,\,A-1\,,\,1\,,\,-B-1\,,\,-\beta\,],\end{aligned}$$

and

$$\begin{aligned}[\,\alpha\,,\,A\,,\,B\,,\,\beta\,] &= [\,\alpha\,,\,A\,,\,0\,,\,1\,,\,-1\,,\,1\,,\,0\,,\,-B\,,\,-\beta\,]\\ &= [\,\alpha\,,\,A+1\,,\,-1\,,\,-B+1\,,\,-\beta\,].\end{aligned}$$

Proof. The first is just the expansion:

$$\begin{aligned}[\,-\gamma\,] &= [\,0\,,\,-1/\gamma\,] = [\,0\,,\,-1\,,\,\gamma/(\gamma-1)\,]\\ &= [\,0\,,\,-1\,,\,1\,,\,\gamma-1\,] = [\,0\,,\,-1\,,\,1\,,\,-1\,,\,1/\gamma\,] = [\,0\,,\,-1\,,\,1\,,\,-1\,,\,0\,,\,\gamma\,];\end{aligned}$$

now multiply by -1 to get the second claim. ∎

Corollary 5.

$$[\,A+x\,,\,\beta\,] = [\,A\,,\,1/x\,,\,-x^2\beta - x\,] \quad \textit{and} \quad [\,A\,,\,x\,,\,\beta\,] = [\,A+1/x\,,\,-x^2\beta - x\,].$$

Proof. Just note that

$$[\,x+A\,,\,\beta\,] = x[\,1+A/x\,,\,x\beta\,] = x[\,A/x\,,\,1\,,\,-x\beta-1\,] = [\,A\,,\,1/x\,,\,-x^2\beta - x\,],$$

and similarly for the second claim. ∎

3.2. We now return to the calculation of the continued fraction expansion for F. Sequentially we get

$$
\begin{aligned}
F &= [\, aX^{-1} \,,\, \tfrac{1}{b}X^2 - \tfrac{c}{b^2}X + \tfrac{c^2-bd}{b^3} \,,\, \beta \,] \\
&= [\, aX^{-1} \,,\, \tfrac{1}{b}X^2 - \tfrac{c}{b^2}X \,,\, \tfrac{b^3}{c^2-bd} \,,\, -\tfrac{(c^2-bd)^2}{b^6}\beta - \tfrac{c^2-bd}{b^3} \,] \\
&= aX^{-1}[\, 1 \,,\, \tfrac{a}{b}X - \tfrac{ac}{b^2} \,,\, \tfrac{b^3}{a(c^2-bd)}X \,,\, a\beta'/X \,] \\
&= aX^{-1}[\, 0 \,,\, 1 \,,\, -\tfrac{a}{b}X + \tfrac{ac}{b^2} - 1 \,,\, -\tfrac{b^3}{a(c^2-bd)}X \,,\, -a\beta'/X \,] \\
&= aX^{-1}[\, 0 \,,\, 1 \,,\, -\tfrac{a}{b}X \,,\, \tfrac{b^2}{ac-b^2} \,,\, \tfrac{(ac-b^2)^2}{b^4}\tfrac{b^3}{a(c^2-bd)}X - \tfrac{ac-b^2}{b^2} \,,\, \tfrac{ab^4}{(ac-b^2)^2}\beta'/X \,] \\
&= aX^{-1}[\, 0 \,,\, 1 \,,\, -\tfrac{a}{b}X \,,\, \tfrac{b^2}{ac-b^2} \,,\, \tfrac{(ac-b^2)^2}{b^4}\tfrac{b^3}{a(c^2-bd)}X \,,\, -\tfrac{b^2}{ac-b^2} \,,\, -a\beta'/X + \tfrac{ac-b^2}{b^2} \,] \\
&= [\, 0 \,,\, \tfrac{1}{a}X \,,\, -\tfrac{a^2}{b} \,,\, \tfrac{b^2}{a(ac-b^2)}X \,,\, \tfrac{(ac-b^2)^2}{b(c^2-bd)} \,,\, -\tfrac{b^2}{a(ac-b^2)}X \,,\, -a^2\beta'/X^2 + \tfrac{a(ac-b^2)}{b^2}/X \,] \\
&= [\, 0 \,,\, \tfrac{1}{a}X - \tfrac{b}{a^2} \,,\, -\tfrac{a^3}{ac-b^2}X + \tfrac{a^2}{b} \,,\, -\tfrac{b(ac-b^2)^2}{a^4(c^2-bd)} \,,\, \tfrac{a^3}{ac-b^2}X \,,\, \tfrac{b^2}{a^2}\beta'/X^2 - \tfrac{ac-b^2}{a^3}/X \,] \\
&= [\, 0 \,,\, \tfrac{1}{a}X - \tfrac{b}{a^2} \,,\, -\tfrac{a^3}{ac-b^2}X + \tfrac{a^2}{b} - \tfrac{a^4(c^2-bd)}{b(ac-b^2)^2} \,,\, \ldots],
\end{aligned}
$$

which, *mirabile dictu*, is as we had expected and had asserted.

Note that the second expansion (4) contains more information than the first (3), whence my reluctance to work from the first expansion. Note also that the computation just presented is not the sort of thing one will essay more than once in a lifetime. Indeed, other than over the finite field $\mathbb{F}_2$, and perhaps $\mathbb{F}_3$, it surely cannot be reasonable to attempt to obtain detailed information in this way in general circumstances. Over those finite fields, on the other hand, the methods just illustrated may be pursued without pain or fear; for example, there is work of Niederreiter and Vielhaber [8, 9] applying just these notions. Note also the pursuit of the present ideas over $\mathbb{Z}$ in a very special case [7], and mention of similar such cases in [10].

4. Applications

4.1. Denote by $D(X)$ a monic polynomial of even degree $2g+2$ defined over $\mathbb{Z}$. Contrary to the numerical case, the continued fraction expansion of $\sqrt{D}$ is *not* periodic in general. Indeed, one proves the existence of a unit in $\mathbb{Q}(\sqrt{D})$, equivalently periodicity of the expansion, by the box principle. But there are infinitely many polynomials of bounded degree with coefficients in an infinite field. It is easy to see that the partial quotients a_h of $\sqrt{D}$ satisfy $\deg a_h \le g$ unless the expansion happens to be periodic in which case the occurrence of a partial quotient of degree $g+1$ signals the end of a quasi-period.

For example (see [11]) it happens that

$$
\begin{aligned}
&\sqrt{X^4 - 2X^3 + 3X^2 + 2X + 1} = \\
&[X^2 - X + 1 \,,\, \overline{\tfrac{1}{2}X - \tfrac{1}{2} \,,\, 2X - 2 \,,\, \tfrac{1}{2}X^2 - \tfrac{1}{2}X + \tfrac{1}{2} \,,\, 2X - 2 \,,\, \tfrac{1}{2}X - \tfrac{1}{2} \,,\, 2X^2 - 2X + 2}\,]
\end{aligned}
$$

is periodic whereas

$$\begin{aligned}
\sqrt{D} &= \sqrt{X^4-2X^3+3X^2+2X+2}\\
&= \Big[X^2-X+1\,,\ \tfrac{1}{2}X-\tfrac{5}{2^3}\,,\ \tfrac{2^5}{3\cdot7}X-\tfrac{2^3\cdot43}{3^2\cdot7^2}\,,\ -\tfrac{3^3\cdot7^3}{2^8\cdot31}X-\tfrac{3^2\cdot7^2\cdot6719}{2^{11}\cdot31^2}\,,\\
&\quad -\tfrac{2^{14}\cdot31^3}{3^4\cdot7^4\cdot13229}X+\tfrac{2^{11}\cdot5^2\cdot31^2\cdot329591}{3^4\cdot7^4\cdot13229^2}\,,\ -\tfrac{3^3\cdot7^3\cdot13229^3}{2^{17}\cdot5\cdot31^4\cdot1877}X+\tfrac{3^2\cdot7^2\cdot13229^2\cdot21577726507}{2^{19}\cdot5^2\cdot31^4\cdot1877^2}\,,\\
&\quad -\tfrac{2^{21}\cdot5^3\cdot31^4\cdot1877^3}{3\cdot7\cdot11\cdot13229^4\cdot12524251}X-\tfrac{2^{19}\cdot5^2\cdot31^4\cdot47\cdot1877^2\cdot2693\cdot1180897}{3^2\cdot7^2\cdot11^2\cdot13229^4\cdot12524251^2}\,,\\
&\quad +\tfrac{11^3\cdot13229^4\cdot12524251^3}{2^{25}\cdot5^4\cdot31^5\cdot1877^4\cdot130960463}X-\tfrac{11^2\cdot13229^4\cdot2109269\cdot12524251\cdot208276252871}{2^{29}\cdot5^3\cdot31^6\cdot1877^4\cdot130960463^2}\,,\\
&\quad \tfrac{2^{33}\cdot5^4\cdot31^7\cdot1877^4\cdot130960463^3}{3^2\cdot7\cdot11^4\cdot67\cdot331\cdot13229^4\cdot12524251^4\cdot32646599}X\\
&\qquad -\tfrac{2^{29}\cdot5^4\cdot31^6\cdot1877^4\cdot130960463^2\cdot672668401\cdot6280895711017969}{3^4\cdot7^2\cdot11^4\cdot67^2\cdot331^2\cdot13229^4\cdot12524251^4\cdot32646599^2}\,,\\
&\qquad \ldots\ldots\Big]
\end{aligned}$$

seemingly is not.

On the other hand, if we were to view D as defined over some finite field, say $\mathbb{F}_p$ (with $p\neq2$), then necessarily its expansion must be periodic because now there are only finitely many polynomials of bounded degree. Indeed, inspection of the expansion above shows that the partial quotient a_2 blows up at $p=3$ and at $p=7$, a_5 blows up at $p=5$, a_6 at $p=11$, … signalling period length $r=2$ at $p=3$ and $p=7$ (more to the point: regulator, the sum of the degrees of the partial quotients making up a quasi-period, $m=3$ at those primes), regulator $m=6$ at $p=5$, regulator $m=7$ at $p=11$, … . This more than suffices, by a remark of Jing Yu [15], to *prove* that the expansion of $\sqrt{D(X)}$ over $\mathbb{Q}$ is indeed not periodic.

Specifically, Yu points out that, by the reduction theory of abelian varieties, if a divisor class (here, that of the divisor at infinity) is of order m on the Jacobian $\operatorname{Jac}\mathcal{C}$ of some curve $\mathcal{C}$ then unless $p\mid m$, it is also of order $m_p=m$ on $\operatorname{Jac}\mathcal{C}_p$, the Jacobian of the curve $\mathcal{C}$ reduced modulo a prime p of good reduction for $\mathcal{C}$; if p divides m then $m=m_pp^i$, some positive integer i. For our example $m_7=3$ and $m_5=6$ suffices to prove non-periodicity. We should here note that the primes dividing the discriminant of the polynomial $X^4-2X^3+3X^2+2X+2$ are 2, 3, and 31 so both 7 and 5 are primes of good reduction.

4.2. Suppose one hopes to find all quartics whose square root *does* have a periodic expansion. Without too much loss, denote the general quartic D by

$$D(X)=(X^2+u)^2+4v(X+w);$$

here one may also usually suppose the normalisation $u+w^2=v$. It turns out not to be impossibly painful [12] to compute the partial quotients $a_0(X)=X^2+u$, …, $a_h(X)=2(X-c_h)/b_h$, by

$$b_{2h}=\frac{s_3s_5\cdots s_{2h-1}}{s_2s_4s_6\cdots s_{2h}}\quad\text{and}\quad b_{2h+1}=4v\frac{s_2s_4s_6\cdots s_{2h}}{s_3s_5\cdots s_{2h+1}}\tag{5}$$

and

$$c_{h+1}=(-1)^h\big(w-s_2+s_3-s_4+\cdots+(-1)^hs_{h+1}\big),\tag{6}$$

where

$$s_{h+1}=v/s_h(s_h-1)s_{h-1}\quad\text{for } h=3,\ 4,\ \ldots,$$

and $s_0=0$, $s_1=\infty$, $s_2=1$, $s_3=v/(1-2w)$.

One finds that the specialisation $b_{m-1}=0$, equivalently $s_{m-1}=\infty$, signals that $a_{m-1}(X)$ blows up (to degree 2), implying regulator m. In the case of periodicity, the 'symmetry' $s_1=s_{m-1}$ in fact implies that $s_2=1=s_{m-2}$, $s_3=s_{m-3}$, ...

The case $m=2$ is $v(X+w)=\kappa$, some constant; $m=3$ is $u=-w^2$. From there on $u+w^2=v$. Then $m=4$ is $s_3=\infty$ so $1=2w$; $m=5$ is $s_3=1$ or $v=1-2w$; $m=6$ is $s_4=v/s_3(s_3-1)=1$; $m=7$ is $s_4=s_3$ or $v=s_3^2(s_3-1)$; $m=8$ is $s_5=s_3$, where in fact $s_5=(s_3-1)/(s_4-1)$, and so on.

Indeed, one obtain a raw form of the modular equation defining $X_1(m)$. For example the condition $s_6=s_5$ for $m=11$ quickly simplifies to

$$s_3(s_3-1)=s_5^2(s_5-1).$$

See [12] for details or, for different methods to construct the families of curves, [6], [2], or [13]; the original tabulation occurs in [5], see also [4].

4.3. The case $g=2$, thus the issue of the periodicity of the continued fraction expansion of the square root of a sextic defined over $\mathbb{Q}$, is more interesting if only because, unlike the elliptic case, we do not yet know all possibilities. Preliminary study suggests it is useful to distinguish the cases $D(X)$ given by

$$(X^3+fX+g)^2+u(X^2+vX+w) \quad \text{or} \quad (X^3+fX+g)^2+v(X+w).$$

Generically, after the first several quotients, all partial quotients will be of degree one so, just as in the $g=1$ case, periodicity requires specialisations of — that is, relations on — the coefficients f, g, u, v, w. However, now a 'blowup' of a partial quotient may mean no more than that a multiple of the divisor at infinity on the Jacobian of the hyperelliptic curve $Y^2=D(X)$ is (technically, corresponds to) a point on the curve and, unlike the elliptic case, does not guarantee periodicity. It will be interesting to see whether the Reduction Theorem is helpful in practice in recognising blowup to degree $g+1$.

References

[1] J.-P. Allouche. M. Mendès France, and A. J. van der Poorten, 'An infinite product with bounded partial quotients', *Acta Arith.* **59** (1991), 171–182.

[2] Roberto M. Avanzi and Umberto M. Zannier, 'Genus one curves defined by separated variable polynomials and a polynomial Pell equation', *Acta Arith.* **99**.3 (2001), 227–256.

[3] David G. Cantor, 'On the continued fractions of quadratic surds', *Acta Arith.* **68** (1994), 295–305.

[4] Everett W. Howe, Franck Leprévost, and Bjorn Poonen, 'Large torsion subgroups of split Jacobians of curves of genus two or three', *Forum Math.* **12**.3 (2000), 315–364 (MR2001e:11071).

[5] Daniel Sion Kubert, 'Universal bounds on the torsion of elliptic curves', *Proc. London Math. Soc.* **33**.3 (1976), 193–237.

[6] Abderrahmane Nitaj, 'Détermination de courbes elliptiques pour la conjecture de Szpiro', *Acta Arith.* **85**.4 (1998), 351–376; 'Isogenes des courbes elliptiques definies sur les rationnels', to appear in *J. Combinatorial Math.*; see `http://www.math.unicaen.fr/~nitaj/`.

[7] Michel Mendès France, Alfred J. van der Poorten, and Jeffrey Shallit, 'On lacunary formal power series and their continued fraction expansion', in *Number Theory in Progress* (Proc. Conf. in honour of Andrzej Schinzel on the occasion of his 60th birthday), K. Győry, H. Iwaniec and J. Urbanowicz eds, Walter de Gruyter, Berlin 1999, 321–326.

[8] Harald Niederreiter and Michael Vielhaber, 'Linear complexity profiles: Hausdorff dimensions for almost perfect profiles and measures for general profiles', *J. Complexity* **13**.3 (1997), 353–383.

[9] ———, 'An algorithm for shifted continued fraction expansions in parallel linear time. Cryptography', *Theoret. Comput. Sci.* **226**.1–2 (1999), 93–104.

[10] Alf van der Poorten, 'Formal power series and their continued fraction expansion', in Joe Buhler ed., *Algorithmic Number Theory* (Proc. Third International Symposium, ANTS-III, Portland, Oregon, June 1998), Springer Lecture Notes in Computer Science **1423** (1998), 358–371.

[11] Alfred J. van der Poorten, 'Non-periodic continued fractions in hyperelliptic function fields' (Dedicated to George Szekeres on his 90th birthday), *Bull. Austral. Math. Soc.* **64** (2001), 331–343.

[12] ———, 'Periodic continued fractions and elliptic curves', in *High Primes and Misdemeanours*: lectures in honour of the 60th birthday of Hugh Cowie Williams, Alf van der Poorten and Andreas Stein eds., Fields Institute Communications **42**, American Mathematical Society, 2004, 353–365. See also 'Elliptic curves and continued fractions', `www.arxiv.org/math.NT/0403225` for more on this topic.

[13] Alfred J. van der Poorten and Xuan Chuong Tran, 'Periodic continued fractions in elliptic function fields', in Claus Fieker and David R. Kohel eds, *Algorithmic Number Theory* (Proc. Fifth International Symposium, ANTS-V, Sydney, NSW, Australia July 2002), Springer Lecture Notes in Computer Science 2369 (2002), 390–404.

[14] Wolfgang M, Schmidt, 'On continued fractions and diophantine approximation in power series fields', *Acta Arith.* **95** (2000), 139–166.

[15] Jing Yu, 'Arithmetic of hyperelliptic curves', manuscript marked *Aspects of Mathematics*, Hong Kong University, 1999; see pp.4–6.

ceNTRe for Number Theory Research, 1 Bimbil Place, Killara, Sydney 2071, Australia
E-mail address: `alf@math.mq.edu.au (Alf van der Poorten AM)`